Responses to the hybridised threat landscape

CONCLUSION PAPER

RESPONSES TO THE HYBRIDISED THREAT LANDSCAPE

Thematic Panel 3: New Technologies and the Online Dimension

Working Group of EU Knowledge Hub on Prevention of Radicalisation

1ST Meeting
26-27 March 2025
Brussels, Belgium

EU Knowledge Hub on Prevention of Radicalisation

European Commission

The thematic panel on **New Technologies and the Online Dimension** is a crucial activity of the **EU Knowledge Hub on the Prevention of Radicalisation** (EUKH). The inaugural meeting of March 26th and 27th in Brussels examined the impact of new technologies and the online dimension on the evolving threat landscape, and online radicalisation. The panel focused on three specific topics: the Hybridised Threat Landscape, the Challenges faced by the Frontline Actors, and Vulnerability of Minors and At-Risk Communities. The Conclusion Paper presents the main findings of the three panels: Sections 1 and 2 will address respectively the Key Insights of the topic "Tackling Hybrid Extremism with Precision" and "Safeguarding Minors in the Hybrid Threat Era" while Section 3 is devoted to present the main Takeaways from the two-days panel.

1. Key Insights: Tackling Hybrid Extremism with Precision

The Role of Non-Ideological Violence in Radicalisation: The fascination with non-ideological violence, or nihilistic violence has emerged as a significant driver of online radicalisation. This phenomenon often appeals to individuals seeking a sense of power or identity rather than belief in specific political or religious ideologies. Addressing this issue requires **targeted interventions that focus on the psychological and social factors driving this fascination.**

Combatting the Convergence of Online Harms Across the EU: The growing online cross-over between various harms, such as online sexual abuse material (CSAM) and organised crime, present a significant challenge across the EU. The overlap between organised crime and radicalisation highlights the importance of **addressing these interconnected threats through comprehensive strategies that disrupt recruitment pipelines** and prevent the spread of harmful narratives.

The Influence of Online Personalities in Spreading Extremist Narratives: Influencers and streamers play a pivotal role in the dissemination of conspiracy theories and the radicalisation of mixed ideologies. The discussion focused on the issue of "**influence as a service**" with the aim of **considering online influencers - active in the context of P/CVE - also as a strategic asset** to provide positive interventions (e.g. in gaming spaces and communities).

Decoding Platform Migration and Coded Language in Extremist Tactics: Terrorist groups tend to pervade fringe, and alt-tech social media platforms, leading users in a malicious way, toward more

hyper-partisan and extremist contents typical of the “below-the-radar online environments". Across these spaces, actors use coded language that may be hard to detect without the proper subject-matter expertise and context that is needed to recognise such material as harmful. **Equipping policymakers, practitioners, and content moderators with the knowledge to identify and interpret coded language** is vital to countering these tactics and disrupting the spread of harmful content.

Harnessing AI Chatbots to Counter Online Radicalisation?: The panel discussed the potential of chatbots in dissuading people from adhering to harmful beliefs, as the AI-driven systems can engage individuals exposed to extremist content, **offering alternative narratives and support in real-time**. Studies on this, however, are very limited, with one successful noteworthy by MIT that showed how through the engagement with a chatbot, people’s attitudes towards harmful conspiracies decreased. However, the panel also highlighted **the risk of employing such bots**, as there is a lack of transparency when it comes to the data, a lack of proper guardrails, and the potential for unintended consequences. The effectiveness of such tools depends on **robust oversight** and **continuous evaluation** to ensure ethical use and prevent misuse. As such, according to the panel members, the positive applications of AI must be approached with nuance, as technology still faces significant issues, including **biased algorithms**. **De-radicalisation chatbots** could play a helpful role, but the above-mentioned complexities highlight the need for cautious optimism and **further investigation**.

Fostering Emotional Literacy for Empowered Digital Engagement: Recognising the interconnected nature of the digital ecosystem, the panel advocated for **extending the concept of digital literacy to incorporate emotional literacy, for young people and for broader online audiences**. Digital literacy campaigns need in fact to be tailored to different age groups involving minors as well as adults. **Highlighting successful campaigns and promoting critical thinking skills** were identified as key measures to empower individuals to navigate and challenge harmful online content effectively.

Challenges in Platform Governance and Content Moderation: The panel reflected that online regulation varies significantly across regions, and terrorist actors are exploiting these inconsistencies to their advantage. This disparity highlights **the need for a more inclusive and globally coordinated approach to platform governance, ensuring that moderation practices are equitable and effective** across diverse linguistic and cultural contexts.

Integrating Strategies to Counter Radicalisation, Disinformation, and Foreign Information Manipulation & Interference (FIMI): Disinformation campaigns often serve as a **gateway to radicalisation**, exploiting societal divisions and amplifying extremist narratives. Similarly, FIMI tactics target vulnerabilities within democratic systems, undermining trust and stability.

Collaborative initiatives that **integrate counter-narratives, digital literacy programs, and emotional framing** are essential to mitigate the impact of these intertwined challenges.

2. Key Insights: Safeguarding Minors in the Hybrid Threat Era

Rebuilding Trust: Engaging Minors to Counter Hybrid Threats: Minors face unique risks in online environments, exacerbated by the lack of follow-up on at-risk behavior and their **diminishing trust in traditional institutions**. Instead, they place their trust in **influencers**, who often wield significant sway over their perspectives and decision-making. To **rebuild trust between minors and educational or local institutions**, a multi-faceted approach is essential.

Educational institutions should embrace **multiple digital literacy initiatives**, including modern teaching methods that integrate technology and address issues minors care about, such as online safety and misinformation. **Collaborating** with trusted influencers and youth leaders can amplify these efforts, **bridging the gap between institutions and minors' trusted sources of information**. Furthermore, local institutions can establish mentorship programs and community outreach initiatives, connecting minors to **positive role models** who can guide them away from extremist narratives.

Tackling Toxic Masculinity and Fostering Safe Online Spaces: Toxic masculinity promotes gender-based violence online and offline, resulting into risks to women and girls, non-conforming gender identities, as well as men and boys. Online platforms amplify this issue by **normalising toxic behaviours through memes, videos, and forums that glorify violence** and misogyny. Addressing toxic masculinity and fostering safe online spaces for minors requires a **multi-pronged approach** that involves **education**, **policy changes**, and **community engagement**.

Engaging Youth in P/CVE: Involving youth in P/CVE activities is a **powerful strategy**. By empowering young individuals to take an active role, they become **advocates for positive change within their communities**, fostering resilience against extremist narratives. Additionally, their involvement helps bridge generational gaps, creating a **sense of ownership and trust in P/CVE efforts** (e.g. The project Streetwork@online).[1]

[1] This programme engages youth directly through platforms like Instagram, TikTok, and Discord, offering tailored support and promoting democratic values. By leveraging the insights and creativity of young people, Streetwork@online demonstrates the benefits of involving youth in crafting effective counter-narratives and

From Battlefield to Backyards: Minors' Involvement in Military Groups: The panel highlighted **the emergence of military groups** (e.g. in Poland) **composed of minors** trained by individuals returning from Ukraine and influenced by **fascist and neo-Nazi ideologies promoted in digital spaces**. Those groups shared specific memes, including sexualised anime characters, which serve as a form of coded communication and ideological reinforcement. These memes may also act as a **recruitment tool**, appealing to specific subcultures and interests while subtly embedding extremist ideologies. This phenomenon highlights the intersection of **digital culture and radicalisation**, warranting further exploration into its implications for youth involvement in such groups.

The Impact of Moderation on Minors in Gaming Environments: The panel emphasised the importance of **evaluating moderation activities** in gaming platforms, particularly in the context of minors. These restrictions are often perceived as limitations on free speech or even as a form of censorship: when moderation measures interfere with this experience, **they risk fostering anti-establishment sentiments** not only against governments but also gaming companies enforcing such regulations. This shift in attitudes can create a breeding ground for **resistance to authority and institutional mistrust.** To contrast this tendency the panel **highlighted the importance of a multi-stakeholder collaboration** involving Police, civil society organisations (CSOs) and the gaming platforms as in the case of the Swedish 'Gamingnätverket'.

Understanding Offline-Online Nexus in Youth Radicalisation and the role of Parents: Offline identity factors significantly influence online behaviours and the radicalisation of minors. The panel emphasised the importance of evaluating interventions and addressing vulnerabilities that arise from the intersection between offline and online experiences—a phenomenon referred to as **"onlife radicalisation."** A critical yet recommendation is **the need to focus on parents**: they should be made aware of the hybridised threat landscape, which blurs the lines between various online harms such as extremist content, disinformation, hate speech, and manipulative grooming tactics. By understanding where these harms are most prevalent and the risks they pose, parents can play a proactive role in guiding and protecting their children online. To effectively combat the hybridised threat landscape and the radicalisation of minors, **a comprehensive approach is needed** involving both online and offline dimensions.

fostering a safer digital environment. Such initiatives highlight the importance of youth engagement in addressing the hybridised threat landscape.

Key Takeaways for Responding to Hybridised Threat Landscapes

The following section presents the main conclusions as suggested by the panel's participants as results of the above-mentioned insights. They have to be considered as key-recommendations for future actions to be integrated by the European Commission.

Harnessing Public Vigilance: A Key to Counterextremism Success: Member States (MS) must embrace the power of collective vigilance by establishing **accessible online reporting platforms**. These mechanisms empower citizens to flag suspicious terrorism-related activities, fostering a proactive and united front against threats. Inspired by Australia's successful **"See Something, Say Something"** model and the Spanish initiative "Stop Radicalismos", this approach transforms ordinary individuals into vital contributors to national security. By creating user-friendly and secure channels for reporting, not only enhance public trust but also strengthens their ability to respond effectively to emerging risks. This strategy isn't just about technology—it's about building a culture of **shared responsibility** and **resilience**.

Uniting Expertise: Tackling Hybrid Threats and the Cross-Over of Online Harms Through Multidisciplinary Collaboration: To confront the ever-evolving threat landscape, MS must champion the creation of multidisciplinary teams within **Law Enforcement Agencies (LEAs)** and specifically their **Internet Referral Units (IRUs)**. These teams, composed of experts from various fields, are crucial for identifying and addressing not only traditional threats but also the interconnected and overlapping online harms that span multiple domains, ensuring a comprehensive approach to threat detection and intervention.

Crafting Precision: Tailored Online Strategies to Preventing and Counter Violent Extremism: Member States must prioritise the **development of targeted P/CVE strategies specifically designed for the online domain**. Taking inspiration from the Netherlands' successful implementation, these strategies should address the **unique challenges and opportunities of the digital landscape**. Tailored P/CVE strategies enable MS to combat these dynamics effectively.

Building Resilience Through Digital Literacy: Empowering All Audiences: To tackle the challenges of harmful online content, Member States must prioritise the integration of digital literacy programs into **national curricula** and **employee training initiatives**. These programs should be tailored to **diverse audiences**, equipping individuals with the skills to **navigate platforms critically** and recognise potential threats in the digital sphere. By embedding **digital literacy** into **education systems** and **workforce training**, MS can foster a culture of **informed and responsible online**

engagement. This initiative promotes resilience across **all demographics**—empowering young students, professionals, and communities to safely and confidently interact in the digital age.

Empowering Educators and Mental Health Professionals: Bridging the Knowledge Gap: Member States must establish robust structures and guidelines, including **centralised databases**, to equip educators and mental health professionals with the latest insights into **digital ecosystems, platforms, coded language, and emerging threats**. These resources would ensure that professionals remain **well-informed and capable of addressing the challenges of the modern digital landscape**. P/CVE institutions must **deepen collaboration with ministries of education** to raise awareness among educators about the pressing issue of online harms. This partnership should focus on equipping educators with the knowledge and tools to address challenges such as violence, child sexual abuse (CSA), TVE and online radicalisation. The rapidly changing nature of digital platforms and the subtleties of coded language can make it challenging **to stay ahead of potential online risks**. By creating accessible, **up-to-date knowledge hubs**, MS can empower these professionals to foster safer environments, support vulnerable individuals, and contribute to a proactive defense against digital threats.

Adapting Global Wisdom: Tailoring International Insights for EU Needs: Member States should actively seek out transferable lessons from successful global initiatives, such as Australia's pioneering approaches to combating terrorism and online harm. By critically evaluating these practices and customising them to fit EU-specific needs, MS can strengthen their ability to address the unique challenges facing the region. **Adapting global practices** ensures that MS benefit from proven solutions while considering cultural, legal, and structural differences within the EU. This approach **encourages cross-border collaboration** and **fosters the exchange of knowledge**, enabling the **EU to remain at the forefront of addressing complex and evolving online threats**.

Advancing Research: Unveiling Radical Networks and Addressing Cross-Over Harms: Member States must intensify efforts to conduct comprehensive **research and assessments** to establish clear links between the activities of groups such as 764 and the Order of Nine Angles and terrorism. This research should also focus on **crossover cases** involving grooming, sextortion, TVE propaganda, and radicalisation, leveraging TCO assessments as a critical tool. **The crossover of online harms**—where grooming, sextortion, and propaganda intersect—creates a complex web that demands a nuanced and informed response. By advancing research and utilising TCO assessments, MS can uncover these connections.

Empowering Online Bystanders: Building Skills to Counter Harmful Behaviors: Member States should invest in **civil society organisation (CSO) programmes** designed to cultivate the skills and confidence needed to empower users to intervene effectively in harmful online behaviors. **Harmful online behaviors**—such as bullying, harassment, and the spread of dangerous

ideologies—often persist due to the bystander effect, where individuals hesitate to act. By fostering civic engagement and training users to act decisively, CSO programmes can transform **passive observers** into **active contributors** to safer digital spaces.

Fostering Inclusive Online Spaces - Integrating Gender Perspectives and Community Involvement: There is a growing need to incorporate gender perspectives into analyses while actively engaging parents and communities in the moderation and creation of safer online environments. This approach ensures that diverse experiences and voices are represented in efforts to tackle harmful online behaviours.

Demystifying Algorithms: Empowering Users Against Manipulation: There is a crucial need to raise awareness about how **algorithms function** and the ways they can be **exploited by malicious actors**. Organising informative sessions or similar initiatives can shed light on the mechanics of algorithms, their influence on online content, and the strategies employed to misuse them, enabling users to better understand and navigate digital threats.

Amplifying Collective Impact: Sharing Best Practices to Prevent Violent Extremism: To enhance collective efforts in preventing and countering violent extremism, greater emphasis must be placed on disseminating successful interventions and raising awareness of the Radicalisation Awareness Network (RAN) Best Practices database. With over 200 practices presented during RAN Working Group meetings since 2012, this resource serves as a valuable repository of innovative strategies and lessons learned.

Annex

Existing Practices

Several successful programs have already implemented in different areas of P/CVE which can be considered as "**reference models**" or "**best practices**". They would be particularly useful to build from past initiatives and to take advantage of the positive outcomes of the different experiences. What follows represents a non-exhaustive list of cases addressed by the participants during the panel discussion.

The "**Stop Radicalismos**" initiative, launched by Spain's Ministry of the Interior, is a collaborative effort to combat radicalisation and violent extremism. It provides citizens with secure and confidential channels to report potential cases of radicalisation, whether involving individuals or groups. Through its website, mobile application, and dedicated hotline, the initiative encourages public participation in identifying and preventing extremist behaviours.

The inclusion of **Preventing and Countering Violent Extremism (P/CVE) in the municipality of Valencia**, Spain, represents a best practice that could serve as an inspiring model for other local authorities in Europe. Valencia's transversal plan for coexistence highlights the importance of addressing radicalisation and social cohesion at the municipal level, where interventions can be tailored to the unique needs and circumstances of the community. Local-level initiatives like Valencia's are essential because they foster direct engagement with residents, enabling a deeper understanding of the vulnerabilities that contribute to extremism.

The "**Memory and Prevention of Terrorism**" educational project by Spain's Ministry of the Interior is a significant initiative aimed at raising awareness and fostering resilience among secondary school students. It includes seven units of work designed to address various aspects of terrorism, such as its history, psychological traits, and societal impact. These units integrate subjects like Geography, History, Psychology, and Citizenship, providing educators with comprehensive tools to implement in classrooms.

Sweden's decision to follow the example of Belgium and Denmark and establish a national **Internet Referral Unit** under the Swedish Cyber Crime Center and Police Authority marks a pioneering step in combating online radicalisation. This demonstrates a proactive and comprehensive approach to addressing the growing threats posed by extremist content online. The establishment of this unit is a commendable practice, as it bridges the gap between prevention and enforcement. The Swedish IRU has a multidisciplinary capacity due to its broader mission to address illicit content in various crime areas. This approach is believed to mitigate some of the challenges posed by the hybridised online threat environment. This initiative sets an

inspiring precedent for other EU member states, emphasising the importance of national-level strategies to complement broader European efforts in countering violent extremism online.

The Swedish Police's involvement in the national 'Gamingnätverket' network—coordinated by **the Swedish Center for Preventing Violent Extremism**—together with civil society organisations (CSOs) and gaming platforms highlights the crucial role of multistakeholder collaboration in tackling complex challenges such as the link between gaming and extremism. This collaboration acknowledges the diverse perspectives of stakeholders—ranging from law enforcement to gaming industry representatives—on the risks present in gaming ecosystems. Similarly, the Spanish, Belgian, Irish, Danish and Kosovan Police's involvement in initiatives like the GEMS project highlights the value of proactive engagement in safeguarding digital spaces. At the EU level, **the European Network against Gaming Related Extremism (ENgaGE)** serves as a model for fostering **coordinated situational awareness (CSA)** by uniting stakeholders under a shared understanding of extremist risks in online gaming platforms.

The **INDEED project**, which provides tools for evaluating projects. The INDEED Project focuses on enhancing the evaluation and design of initiatives aimed at preventing and countering violent extremism and supporting de-radicalisation efforts. It provides resources, training materials, and evidence-based tools to empower practitioners, policymakers, and researchers working in this field. One of its key contributions is the evaluation tool, which offers a structured approach to planning and conducting evidence-based evaluations.

Further Readings and References

An intense of work has already been done in recent years by the European Commission in the context of P/CVE and it's important to spread awareness on existing knowledge which can be useful for practitioners when designing programmes. What follows is a non-exhaustive but exemplary list of resources easily accessible online.

The RAN resources, which offer valuable insights into the work conducted on the online dimension. It serves as a comprehensive resource for practitioners, policymakers, and researchers working to prevent and counter violent extremism. These materials consolidate insights, lessons learned, and recommendations from various working groups and expert meetings.

The **RAN/EUKH Collection of Inspiring Practices** features a curated selection of over 200 initiatives dedicated to preventing and countering violent extremism. These practices have been presented and discussed during various RAN Working Group meetings since 2012, offering

valuable insights and strategies for addressing radicalisation and fostering resilience within communities.

The **Strategic Orientations** outlines the European Commission's approach to preventing radicalisation for the years 2024-2025. It builds on previous strategies while addressing emerging challenges and threats.

The **ProtectEU strategy**, the EU's internal security strategy which has been released on 1 April 2025, announces a new toolbox to prevent radicalisation and the development of a new EU Agenda on preventing and countering terrorism and violent extremism. Until this new CT P/CVE paper is published the EU's approach is set out in the **2020 Counter-Terrorism Agenda** which focuses on anticipating, preventing, protecting, and responding to terrorist threats.

The reading list below is a curated selection of resources compiled from two primary sources. Firstly, it includes materials chosen by the Secretariat and Co-leaders to secure informative discussions during the first meeting of the panel members. Secondly, it features publications referenced by participants during the event. The list comprises a mix of academic research published by various institutions and journals, as well as official reports issued by governmental and non-governmental organisations. These materials provide insights into the evolving threat landscape, the role of online spaces and new technologies in radicalisation, and strategies for countering extremism. Together, they form a well-rounded foundation for discussion on security challenges, policy approaches, and practical interventions.

Hybridised Threat Landscape and the role of online dimension

- "Beyond Definitions: The need for a comprehensive human rights-based UK extremism policy strategy"
- "The Impact of technology on radicalisation to violent extremism and terrorism in the contemporary security landscape".
- "Extremism and the internet of the future: Far-right NFTs on Web3".
- "Considerations of the impacts of generative AI on online terrorism and extremism".
- "AI or Aryan Ideals? Part Two: A thematic content analysis of white supremacist engagement with generative AI: Discourse".
- "Durably reducing conspiracy beliefs through dialogues with AI"
- "Social media and its impact on terrorism and violent extremism in the next 2-5 Years".
- "Generative AI and the German far right: Narratives, tactics and digital strategies".
- "The denazify lie. Russia's use of extremist narratives against Ukraine".
- "Conflict amplified: Disinformation and hate in the Israel-Hamas war".
- "Online misinformation during extreme weather emergencies: short-term information hazard or long-term influence on climate change perceptions?".
- "Hate and extremism on gaming platforms".

- "The politics of consuming war: video games, the military-entertainment complex and the spectacle of violence".
- "Durably reducing conspiracy beliefs through dialogues with AI"

Challenges for policymakers and frontline practitioners

- "Playbook on positive intervention strategies online".
- "Implementing positive gaming interventions: A toolkit for practitioners".
- "Handbook on preventing and combating radicalisation among youngsters in Europe".
- "Handbook on measuring and evaluating incident response online".
- "Prevent, detect, and react: A framework for countering violent extremism on gaming surfaces".
- "Online radicalisation: Understanding the online/offline nexus".
- "European Union Terrorism Situation and Trend report 2023 (TE-SAT)".

Vulnerabilities and grooming tactics in the Hybridised Threat Landscape

- "Extreme right radicalisation of children via online gaming platforms".
- "Education in Preventing and Countering Violent Extremism (P/CVE) among the youth".
- "Children's involvement in terrorist and extremist groups. Advanced sciences and technologies for security applications".
- "Drivers of radicalisation? The development and role of the far-right youth organisation 'Young Alternative' in Germany".
- "Exploring driving factors underlying jihadist radicalisation among youth".